



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/627,733

07/28/2003

Jun Iwasaki

240894US6

3800

22850

7590

11/18/2008

OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C.  
1940 DUKE STREET  
ALEXANDRIA, VA 22314

EXAMINER

HOMAYOUNMEHR, FARID

ART UNIT

PAPER NUMBER

2439

NOTIFICATION DATE

DELIVERY MODE

11/18/2008

ELECTRONIC

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com  
oblonpat@oblon.com  
jgardner@oblon.com

<b>Office Action Summary</b>	<b>Application No.</b> 10/627,733	<b>Applicant(s)</b> IWASAKI, JUN	
	<b>Examiner</b> Farid Homayounmehr	<b>Art Unit</b> 2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 12 August 2008.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1,3,5-7,9,11-13,15,16 and 18-20 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1, 3, 5-7, 9, 11-13, 15, 16, 18-20 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                     | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____  | 6) <input type="checkbox"/> Other: _____                          |

### DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 8/12/2008 has been entered.

This action is responsive to communications: application, filed 7/28/2003; amendment filed 8/12/2008.

2. Claims 1, 3, 5-7, 9, 11-13, 15, 16, 18-20 are pending in the case. Claims 2, 4, 8, 10, 14, 17, and 21 were cancelled.

### *Response to Arguments*

3. With respect to rejection of amended claim 1, applicant argues: "However, the cited portion of Shurts fails to disclose any sort of configuration in which a plurality of transmission system are used to receive data, much less that the system **"sets a higher security level for data received through a relatively secure communication path**

Art Unit: 2439

**and a lower security level for other received data....,"** as recited in amended independent Claim 1."

However, first, as indicated in rejection of claim 1, it is the combination of Timmer and Shurts that teaches the limitations of claim 1. Timmer is clearly directed to a plurality of transmission systems used to receive data. Second, Shurts teaches setting higher security levels to more sensitive data and lower security level to less sensitive data. Therefore, in the system of Timmer in view of Shurts, which receives and transmits data, and assigns high security level to more sensitive data, It is only logical to assign a higher level of security to the data received in a secured communication path. It would be obvious and logical to the one skilled in art that the data received in a secured channel is more sensitive than data received in a regular channel. Based on teaching of Shurts, that more sensitive data gets higher security, the data received in a secured channel will be assigned higher security.

Applicant further cites only a portion of Shurts col. 1 line 1 to col. 2 line 5, and argues:

"Thus, the cited portion of Shurts merely describes that a subject's sensitivity level is compared against a sensitivity level of an object being accessed in order to determine whether the subject may have a label that dominates the object. Shurts, therefore, does not describe that the object receives data via a plurality of communication paths having different security levels, whatsoever." However, Shurts col. 1 line 1 to col. 2 line 5 clearly shows an

Art Unit: 2439

example of an object (user login account) gets configured with a clearance or sensitivity level. Therefore, each data item (object) is assigned a security level to be used to enforce access control. As mentioned above, the combination of Timmer and Shurts teaches receiving data from a communication path and enforcing security. The security level assigned to each object is based on the sensitivity of the object, and therefore, Timmer in view of Shurts teaches **"sets a higher security level for data received through a relatively secure communication path and a lower security level for other received data..."** as required by claim 1.

Applicant further argues that there is no rationale for the statement that "...more sensitive data is transmitted in more secured transmission system. However, the purpose of a more secured transmission system is to protect sensitive data. Secured transmission is more costly than regular transmission. If there is no sensitivity associated with the data to be transmitted, there is no reason to use the more costly secured transmission system.

Applicant further argues the sensitivity of data is defined by the data itself, and not based on communication path via which the data is transmitted. However, at the receiving end, the data itself does not identify its sensitivity. It is the communication path that provides an indication whether data is sensitive or not. The more secured path delivers more sensitive data.

With regards to claims 13, 16 and 20, applicant argues that the feature of "compare the acquired metadata and display the result of comparison" is not taught in claim 1, and therefore not taught by the references. However, claim 1 includes the limitation of: "supplies, in response to an external access request, metadata from metadata storage unit that matches a security level available to the external access request." This limitation includes matching (comparing) the metadata. It also includes supplying the metadata based on the result of the comparison, which teaches displaying the result of the comparison. The rejection of claim 1 shows how the prior art teaches requirement of claim 1, and therefore, as indicated in their associated rejections, does the same for claims 13, 16 and 20.

Based on the discussion above, applicants argument relative to allowability of the pending claims is found non-persuasive.

### ***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1, 3, 5-7, 9, 11-13, 15, 16, 18-20 rejected under 35 U.S.C. 103(a) as being unpatentable over Timmer (U.S. Patent Application Publication No. 2002/0107895, filed Aug. 3, 2001), and further in view of Shurts (U.S. Patent No. 5,572,673, dated Nov. 5, 1996).

5.1. As per claim 1, Timmer is directed to a mobile information communication device, which supports information exchange and fostering of human relations between a plurality of users, (The "Host" as described in parag. 4 of Timmer, and parag. 18-21, where a PDA (mobile device) stores a user personality book), comprising: a wireless communication unit which transmits and receives wireless communication data (Timmer parag. 31 suggests use of wireless application to exchange data in one of the example embodiments. Also see parag. 27, suggesting the device storing the book to be a cellular device); a metadata storage unit which stores, in the mobile unit, metadata relating to activities and interests of a user of the communication device (parag. 4-6 indicating that the data is stored in the Host. Parag. 28-33 shows examples of data related to user interests and activities); and a central control unit which manages the storage of metadata in said metadata storage unit (Timmer parag. 19 teaches database systems to be used to manage the data to be stored in the Host), wherein said central control unit partitions said metadata storage unit by security level and category, stores metadata received through said radio communication unit in a corresponding partition of the metadata storage unit based on matching the received metadata with a security

Art Unit: 2439

level and/or category predetermined by the user (enforcing security based on assigned levels and categories to data in a database management system was well known and widely practiced at the time of invention. However, Timmer does not explicitly talk about details of enforcing security. Shurts explains the enforcement of MAC rules using labels in col. 1, line 52 to col. 2 line 5. Shurts specifically defines security levels and categories in col. 4, line 55 to col. 5, line 51, and particularly in col. 5 lines 7-20. MAC rules are typically implemented in Operating Systems and allow secure storage and access of data based on the labels assigned to data. Therefore, in Shurts system, each data object receives a label (level and/or category), which is used to determine if access to data object is allowed or not. Therefore, each data object is stored based on the assigned security label, and in a portion of metadata storage that corresponds to the assigned label. Details related to combination of the arts taught by Timmer and Shurts is described below),

and sets a higher security level for data received through a relatively secure communication path and a lower security level for other transmitted data (as explained in col. 1 line 53 to col. 2 line 5, the more sensitive data gets a higher level or category. The more sensitive data is typically transmitted in the more secured transmission system. Therefore, data received in a more secured transmission system is typically more sensitive data. Also see response to arguments above, explaining that it would be logical to assign higher security level to more sensitive data).



supplies, in response to an external access request, metadata from the metadata storage unit that matches a security level available to the external access request (As mentioned above, Shurts suggests deployment of MAC rules to enforce security, which supplies data to a requestor only if the level and/or category of the requestor matches that of the requested data), and wherein said metadata is information in the form of metadata, equivalent to a log providing information on locations visited by the user (Shurts is directed to a secured database system and the purpose of databases is storing linked pieces of information such as the user, its visits and the visited place. A system capable of storing data related to a user is well capable of storing the information of locations visited by the user. In other words, barring any unexpected result, a person skilled in art would have store[d] the data indicating location visited by a user if an application requires such data. In addition, Timmer paragraph 31 clearly shows storing locations visited by the user).

It would have been obvious to a person skilled in art, at the time the invention was made, to combine Timmer's system with Shurt's system. This is because Timmer uses databases in the system development as mentioned in paragraphs 19 and 25, therefore its system incorporates the art that is analogous to Shurts' art, which builds a database management system to secure data objects (abstract). Furthermore, Timmer stores personal data, which requires privacy protection. As mentioned in paragraph 2, Timmer uses a secured server and makes its data available over the Internet and via

Art Unit: 2439

wireless systems. Therefore the skilled artisan that makes Timmer's system would be motivated to use Shurts' secured database system.

Therefore, it would have been obvious to a person skilled in the art to use Shurts' secured database management system in development of Timmer's system.

5.2. Claims 2, 8, 14 and 17 cancelled by the applicant.

5.3. As per claim 3, the combination of Shurts and Timmer is directed to the information communication device according to claim 1, further comprising: a user input unit for the user of the device to write metadata directly into said metadata storage unit (Shurts col. 14 lines 5-15 describes a key which allows user enter user data).

5.4. Claim 4 is cancelled by the applicant.

5.5. As per claims 5 and 11, Timmer and Shurts are directed to the information communication device according to claim 1. Timmer teaches a virtual person growing means which grows a virtual person corresponding to the user based on the user's history information accumulated in said metadata storage unit. This is because Timmer is directed to an interactive personalized book, which provides users with the ability to record and guide their own physical or emotional transformations over time, or collect and archive content that reflects a specific period of time of their lives. An on-line

Art Unit: 2439

personal history diary, and evolution of personality and life style is possible parag. 9.

Also as shown in parag 29-30, Timmer's system supports, for example, a

"MYLIFEBOOK" which reflects a personalization process corresponding to a person. As mention in parag 29, the personalization tool is interactive and matures as it collects more history data about the person.

5.6. As per claim 6, the combination of Shurts and Timmer is directed to the information communication device according to claim 1, further comprising: a format setting unit which converts the format of metadata taken out of said metadata storage unit as requested by a requesting party (according to Shurts col. 5 lines 40 to 55, the database maybe queried using different languages, and therefore it is formed in the format requested by a requesting party).

6. Claims 7, 9, 11-13, 15, 16, 18-20 are substantially the same as claims 1, 3, 5 and 6 above, Note that Timmer supports exchanging emails and Shurts creates a bidirectional communication (col. 14 line 16-30), and therefore both are capable of receiving and transmitting data. Also note that Timmer paragraph 6-12 teaches that the Host can be updated and also that the information can be accessible on line and from any location where the appropriate hardware is available. Also, Examiner takes the official notice that authenticating parties before the parties can communicate was well known and widely practiced at the time of invention. Therefore, it would have been obvious to authenticate parties of communication before they can exchange data.

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farid Homayounmehr whose telephone number is 571 272 3739. The examiner can normally be reached on 9 hrs Mon-Fri, off Monday biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Farid Homayounmehr

Examiner

Art Unit: 2439

/Kambiz Zand/

Application/Control Number: 10/627,733

Page 12

Art Unit: 2439

Supervisory Patent Examiner, Art Unit 2434